



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|------------------------------|------------------------|
| 10/660,981 | 09/12/2003 | Kevin Moore | 60046.0052US01 | 6124 |
| 7590 Hope Baldauff Hartman, LLC Suite 1010 1720 Peachtree Street Atlanta, GA 30309 | | | EXAMINER REZA, MOHAMMAD W | |
| | | | ART UNIT 2436 | PAPER NUMBER |
| | | | MAIL DATE 06/03/2009 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/660,981

Applicant(s)

MOORE, KEVIN

Examiner

MOHAMMAD W. REZA

Art Unit

2436

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 March 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 and 15-21 is/are pending in the application.
- 4a) Of the above claim(s) 16-19 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13, 15, 20 and 21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in response to the arguments filed on 03/02/2009.
2. Claims 1-13, and 15-21 are pending in the application.
3. Claims 16-19 have been withdrawn.
4. Claims 1-13, 15, and 20-21 have been rejected.

Response to Amendment

5. The examiner withdraws the specification objection as the claim has been cancelled.
6. The examiner withdraws the 101 rejection as the claim has been cancelled.
7. The examiner approves cancellation of claim 14.

Response to Arguments

8. Applicant's arguments filed on 03/02/2009 have been fully considered but they are not persuasive.

Regarding independent claim 1, applicant argues that Schwartz does not disclose, "determining from the data storage device identifiers whether the data storage device supports the security features and is locked". Examiner respectfully disagrees. Indeed, Schwartz teaches during the initial booting of the power on test process the identifier (password) of the memory has been used to determine whether the BIOS proceeds to boot or in a locked configuration (col. 3, lines 1-14). This is exactly the same teaching of applicant's invention (page 12, lines 17-21). Additionally, he also teaches that the identifier of the motherboard plays a role to determine the device is locked (col. 4, lines 1-12). Therefore, it teaches that from the identifier of the device, it determines whether it

is locked. The identifiers is the serial number, password or other type of identifying number of the hard drive which assures the device is secure and authenticated (col. 3, lines 15-18, col. 4, lines 50-65). This simply emphasis the teaching of the claim limitation that determining from the device identifier whether the device supports the security features. Schwartz discloses the data storage device is returning from a powered off state or hardware reset (col. 1, lines 51-60, col. 3, lines 5-65, col. 4, lines 12-25). This discloses the claim limitation, "in response to determination that the data storage device supports the security features and is locked, determining whether the data storage device is returning from a powered off state or a hardware reset". Thus the argument is traversed and sustains the claim rejection.

Regarding independent claim 20, Schwartz discloses the claim limitation "in response to determining that the data storage device is locked, determining whether the data storage device is returning from a sleep state" (col. 1, lines 51-60, col. 3, lines 5-65, col. 4, lines 12-25). Therefore, all the arguments have been traversed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-13, 15, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwartz (US patent 7,100,036) in view of Morisawa et al hereafter Morisawa (US Patent 5,537,544).

11. As per claim 1, and 15 Schwartz discloses a method, and storage medium comprising: reading from each of the data storage devices within the computer one or more data storage device identifiers; determining from the data storage device identifiers whether the data storage device supports the security features and is locked; in response to determining that the data storage device supports the security features and is locked, determining whether the data storage device is returning from a powered off state or a hardware reset (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65). Although, Schwartz discloses the data storage device is returning from the locked and powered off state. He does not expressly discloses in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset, receiving from a user a password for unlocking the data storage device; in response to receiving the password, determining whether the received password is the security password; and in response to the received password being the security password, unlocking the data storage device and thereby allowing access to data stored on the data storage device. However, in the same field of endeavor, Morisawa discloses in response to determining that the data storage device supports the security features and is locked, determining whether the data storage device is returning from a powered off state or a hardware reset; in response to determining that the data storage device is locked and returning from a powered off

state or a hardware reset, receiving from a user a password for unlocking the data storage device; in response to receiving the password, determining whether the received password is the security password; and in response to the received password being the security password, unlocking the data storage device and thereby allowing access to data stored on the data storage device (col. 3, lines 25-67, col. 4, lines 1-10, col. 6, lines 3-39, col. 8, lines 1-40, col. 17, lines 30-55).

Accordingly, it would be obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Morisawa's teachings of receiving the password for unlocking the data storage device with the teachings of Schwartz, for the purpose of suitably using storage device identifier to determine that the storage device status locked and supported the security features.

12. As per claim 2, Schwartz discloses the method wherein the method is implemented during a power on test procedure of the computer hosting the data storage devices (col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40).

13. As per claim 3, Schwartz discloses in response to the received password not being the security password, determining whether limited access should be provided to each locked data storage device (col. 1, lines 51-60, col. 3, lines 1-36, lines 46-67. Schwartz does not disclose wherein; in response to determining that limited access should be provided, setting a bit corresponding to each locked data storage device to exclude the locked data storage device from detection verification during a power on test procedure; and in response to determining that limited access should not be provided to each locked data storage device, isolating each locked data storage device

from the operating system. However, Morisawa discloses wherein; in response to determining that limited access should be provided, setting a bit corresponding to each locked data storage device to exclude the locked data storage device from detection verification during a power on test procedure; and in response to determining that limited access should not be provided to each locked data storage device, isolating each locked data storage device from the operating system (col. 4, lines 1-10, col. 6, lines 3-39, col. 8, lines 1-40, col. 17, lines 30-55).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 3.

14. As per claim 4, Schwartz discloses the method wherein limited access comprises prohibiting reading from or writing to the locked data storage device (Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40).

15. As per claim 5, Schwartz discloses the method wherein in response to the received password being the security password, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67). Schwartz does not disclose in response to determining that the data storage device should be unlocked without requiring a user to enter a password, storing the security password within a memory located outside the data storage device. However, Morisawa discloses in response to determining that the data storage device should be unlocked without requiring a user to enter a password, storing the security password within a memory

located outside the data storage device (col. 4, lines 1-10, col. 6, lines 3-39, col. 8, lines 1-40, col. 17, lines 30-55).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

16. As per claim 6, Schwartz discloses the method wherein in response to determining that the data storage device is locked, determining whether the data storage device is returning from a powered off sleep state; in response to the data storage device being locked and returning from a powered off sleep state, determining whether the data storage device was unlocked prior to the sleep state; in response to determining that the data storage device was unlocked prior to the sleep state, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67). Schwartz does not disclose in response to determining that the data storage device should be unlocked without requiring a user to enter a password, retrieving the security password from the memory and utilizing the security password to unlock the data storage device. However, Morisawa discloses in response to determining that the data storage device should be unlocked without requiring a user to enter a password, retrieving the security password from the memory and utilizing the security password to unlock the data storage device (col. 4, lines 1-10, col. 6, lines 3-39, col. 8, lines 1-40, col. 17, lines 30-55).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 6.

17. As per claim 7, Schwartz discloses the method wherein the security password is stored within the memory in an encrypted format (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67).

18. As per claim 8, Schwartz discloses the method wherein in response to determining that the data storage device should be unlocked after returning from a sleep state by requiring a user to enter a password, receiving the security password from a user and utilizing the security password to unlock the 19. As per claim 9, Schwartz discloses the method wherein in response to determining that the data storage device is unlocked, determining whether a security password has been enabled; and in response to determining that the data storage device is unlocked and that no security password is enabled for the data storage device, disabling, until a next power cycle, the security features that enable security passwords (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67).

20. As per claim 10, Schwartz discloses the method wherein in response to the data storage device being locked and returning from a powered off state or a hardware reset, determining whether a backup password may be used to unlock the data storage device; in response to determining that a backup password may be used, determining whether a request to enter a backup password has been received (Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65); in response to receiving a request to enter a backup password, receiving from a user a password for unlocking the data storage device; and in response to the received password being the backup password, unlocking the data storage device and thereby allowing access to data stored on the

data storage device (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67).

21. As per claim 11, Schwartz discloses the method wherein in response to the received password being the backup password, determining whether a maximum security is supported by the security features; and in response to the received password being the backup password and the maximum security being supported, erasing the data storage device before unlocking the data storage device (Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65).

22. As per claim 12, Schwartz discloses the method in response to determining that the password is not the security password, determining whether the password entry attempt counter is equal to zero (Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65); in response to the password entry attempt counter being greater than zero, decrementing the password entry attempt counter by one and again receiving a password from a user; and in response to the password entry attempt counter equaling zero, prohibiting additional password entries until a next power cycle and displaying a message that the data storage device remains locked (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67).

23. As per claim 13, Schwartz discloses the method wherein executing a setup utility within the basic input/output system operative to control one or more functions for manipulating at least one of a security password and a backup password for a data storage device supporting the security features wherein the functions are accessed by one of entering the security password when prompted by the setup utility and selecting the data storage device in the setup utility when said data storage device is unlocked

(Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65).

24. As per claim 20, Schwartz discloses a method comprising: in response to determining that the data storage device is locked, determining whether the data storage device is returning from a sleep state; in response to the data storage device being locked and returning from a sleep state, determining whether the data storage device was unlocked prior to the sleep state; and in response to determining that the data storage device was unlocked prior to the sleep state, retrieving the security password from the memory and utilizing the security password to unlock the data storage device (col. 1, lines 51-60, col. Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65). Although, Schwartz discloses the data storage device retrieving the security password from memory. He does not expressly discloses storing a security password within a memory located within the computer, but outside the data storage device; in response to determining that the data storage device was unlocked prior to the sleep state, retrieving the security password from the memory and utilizing the security password to unlock the data storage device (col. 3, lines 25-67, col. 4, lines 1-10, col. 6, lines 3-39, col. 8, lines 1-40, col. 17, lines 30-55).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 20.

25. As per claim 21, Schwartz discloses the method wherein the security password is stored within the memory in an encrypted format (Col. 3, lines 1-36, lines 46-67, col. 4, lines 1-40, lines 50-65).

Conclusion

24. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/Mohammad W Reza/
Examiner, Art Unit 2436